PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-259689
(43)Date of publication of application : 22.10.1990

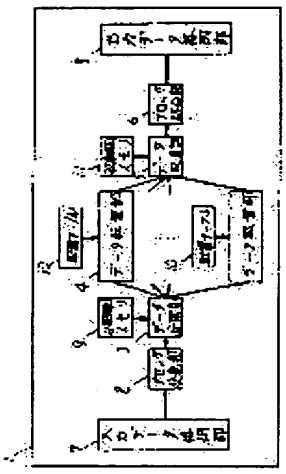
(51)Int.Cl. G09C 1/00

(21)Application number : 01-080351
(22)Date of filing : 30.03.1989

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : HARADA TOSHIHARU
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(54) DATA INVERTER

(57)Abstract:
PURPOSE: To make data decoding practically impossible by grouping data and inverting them for each group.
CONSTITUTION: The data inverter has a means 2 dividing input data series into blocks, a means 3 grouping and arranging data in the same block into several blocks, a means 4 inverting the grouped data in each group, a collecting means 5 collecting the inverted data from each group and arranging them to new blocks, and a block linking means 6 linking the obtained blocks and obtaining the inverted data series. Since the distributing means 3 group and arrange data belonging to each block into several blocks at random, data belonging to each group has no specific relation with original data series, inversion rules for a data inverting means which inverts data for each group cannot be readily estimated.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-259689

⑤1Int.Cl.[5]　識別記号　庁内整理番号　⑬公開　平成2年(1990)10月22日
G 09 C 1/00　7343-5B

審査請求　未請求　請求項の数 1　(全8頁)

⑤4発明の名称　データ転置装置

⑳特　願　平1-80351
㉒出　願　平1(1989)3月30日

⑦2発明者　原田　俊治　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦2発明者　松崎　なつめ　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦2発明者　館林　誠　大阪府門真市大字門真1006番地　松下電器産業株式会社内
⑦1出願人　松下電器産業株式会社　大阪府門真市大字門真1006番地
⑦4代理人　弁理士　粟野　重孝　外1名

明　細　書

1. 発明の名称

データ転置装置

2. 特許請求の範囲

入力データ系列を、ある定められた個数毎のブロックに分割するブロック分割手段と、同一ブロックに属する各データを、定められたある分配規則にしたがって、いくつかのグループに分配し、配置するデータ分配手段と、各グループに分配配置されたデータを、定められたある転置規則に従って各グループ内で転置するデータ転置手段と、各グループにおいて転置されたデータを定められたある収集規則にしたがって新たなブロックに収集し、配置するデータ収集手段と、各ブロックのデータを結合し、転置された出力データ系列を得るブロック結合手段とを備えることを特徴とするデータ転置装置。

3. 発明の詳細な説明

産業上の利用分野

本発明は入力データ系列をある定まった転置規則に従ってそのデータ位置を転置し、異なったデータ系列を出力するデータ転置装置に関する。

従来の技術

データ転置装置は画像・音声・数値データといった各種データの秘密通信に利用される暗号装置の基本構成要素であり、転置規則を秘密の鍵としている。

データ転置装置をハードウェアで構成する場合、高速処理が得られる反面、転置規則が固定的であるため、容易に転置規則が推定され安全性の面で好ましくない。一方マイコン等のソフトウェアで構成する場合、メモリに転置規則を蓄積し、これを更新することで適時転置規則を変化させることができる。従って安全性の問題は解決する。しかし転置処理の速度はハードウェアで構成する場合と比較して遅くなる。また安全性を考慮した転置規則をいかに効率良く生成するかという新たな問題が生じる。

以下ではマイコン等によるソフトウェアで実現したデータ転置装置の従来例について述べる。

従来例1

第3図は従来より広く用いられているデータ転置装置の例である（以下従来例1と称する。例えば特開昭63-53584の従来の技術の項公報）。同図(a)において31は従来例1の構成によるデータ転置装置、32はデータ転置部、33は入力データ格納部、34は出力データ格納部、35は転置規則を格納する転置テーブルである。

この転置装置の動作は以下の通りである。転置すべきN個の入力データ系列は、33の入力データ格納部に一旦格納され、32のデータ転置部に送られる。32のデータ転置部に送られたデータは、そこで35の転置テーブルに従って、そのデータ位置が転置され、34の出力データ格納部に格納される。そして転置された出力データ系列として出力される。

同図(b)は転置テーブルである。従来例1ではN個のデータを転置する大きさの転置テーブルが必要である。転置テーブルの参照はそのアドレスを指定することにより行う。同図に示すように、大きさNの転置テーブルにはそのアドレスi（$1 \leq i \leq N$）のメモリ領域に、i番目の位置のデータの転置すべき位置pi（$1 \leq pi \leq N$）が格納されている。つまりこのテーブルにしたがって、i番目の位置にあったデータはpi番目の位置に転置される。

第4図は従来例1の構成によるデータ転置装置のデータ転置部および転置テーブルの例（この場合N＝10）である。同図(a)は転置テーブル、同図(b)はデータ転置部である。データ転置部では10個のデータが転置テーブルにしたがって、例えば先頭（入力データの1の位置）にあったデータd1は先頭から5番目（出力データの5の位置）に転置され、また先頭から5番目（入力データの5の位置）にあったデータd5は先頭から10番目　（出力データの10の位置）に転置される。

・転置テーブルの容量

転置テーブルに格納されるpi（$\leq N$）を記述するのに必要なメモリ容量は、

$$[\log_2 N] \text{（ビット）}$$

であるので、大きさNの転置テーブルに必要なメモリ容量は

$$M1 = N * [\log_2 N] \text{（ビット）} \quad (1)$$

となる。ここで[a]はa≦bを満たす最小の整数bを表す。具体的に大きさN＝64の転置テーブルには、M1＝384ビットのメモリ容量が必要である。

・転置テーブルの生成

転置規則は以下の条件を満たすように生成される必要がある。（但し条件1は転置規則の生成において満たすべき必要十分条件であるが、条件2)、3)は安全性を高めるための十分条件である。）

条件1）同じ位置に重複して転置されない

pi（$1 \leq i \leq N$、$1 \leq pi \leq N$）はそれぞれ相異なる

条件2）偏りなくランダムに転置される

条件3）全てのデータが転置される（pi≠i）

条件1を実現するため、従来から疑似乱数発生器（N以下の自然数を発生する）を使用して、転置テーブルは生成される。すなわち乱数発生器のN個の出力値pi（$1 \leq i \leq N$、$1 \leq pi \leq N$）がi番目のデータの転置先の位置として転置テーブルに格納される。

これらの条件を満たすため、以下のテーブル生成法が用いられている。

生成法：乱数を1個ずつ発生し、条件を満たす乱数を1個ずつ決定していく。条件を満たさない乱数は棄却し、新たに乱数を発生する。この操作を条件を満たす乱数が得られるまで繰り返す。

この方法ではテーブルの大きさNの増加に伴って、テーブル生成に要する時間が多大となり、かつ生成に要する時間のばらつきが大きくなる。従って限られた時間内に転置テーブルを更新する必要のある場合に、テーブルの大きさNをある程度小さく設定する必要がある。しかし従来例1の構成においてテーブルの大きさNを小さくすることは、次に示す安全性の面から好ましくない。

・安全性

ここでは転置規則を悉皆的に推定し、転置されたデータ系列に対して、逆転置を施して元のデータ系列を復元するという転置規則の解読法に対する安全性について述べる。但しこのような解読が成功するのは、解読者が元のデータ系列に関してなんらかの情報（例えば使用言語、コード等）を知っている場合に限られる。つまり逆転置によってこれらの意味のあるデータが得られることで解読の成否を判定できる場合に限り解読可能となる。

このような解読を現実的に不可能にするため、転置規則を十分大きな母集合の中から選択する必要がある。

従来例１において、選択されるべき転置規則の母集合の大きさは、簡単のために条件１のみを満たす場合を考えると

$$N! \qquad (2)$$

である。Ｎの値を転置規則を推定するのが困難なように、つまり（２）式が十分大きくなるように設定する（但し実際は他の条件をも満たす転置規則の母集合の大きさを十分大きくする）。具体的にはＮ＝３２程度で（２）式が10^{30}以上となり実用上安全となる。

従来例２

第５図にデータ転置装置の第２の従来例を示す（以下従来例２と称する、例えば特開昭６１－１０７３７５公報）。これは入力データ系列をいくつかの小さなブロックに分割し、ブロック単位での転置（ブロック転置）と各ブロック内での転置の２段構成を取っている。このことによりＮ個のデータを転置するのに必要な転置テーブルの大きさを小さくでき、その生成も容易になる。

同図において５１は上記構成によるデータ転置装置であり、以下の各部で構成されている。５２はブロック分割部、５３はブロック転置部、５４は各ブロック毎のデータ転置部、５５はブロック結合部である。また５６は入力データの格納部、５７は出力データの格納部、５８はブロック転置テーブル、５９は各ブロック毎に定められた転置テーブルである。

この転置装置の動作は以下の通りである。転置すべき入力データ系列は、５６の入力データ格納部に一旦格納され、５２のブロック分割部に送られる。ブロック分割部で、分割され、５３のブロック転置部に送られる。ブロック転置部では、５８のブロック転置テーブルに従ってブロック単位でまとめて転置される（各ブロック内でのデータの位置は変わらない）。次にブロック転置された各データは各ブロック毎に５４のデータ転置部に送られ各ブロック毎に５９のデータ転置テーブルに従って各ブロック内で転置される。次に各ブロックの転置されたデータは５５のブロック結合部で結合され、５７の出力データ格納部に格納される。以下ではＮ：データ系列長、Ｌ：ブロック長、ｍ：ブロック数と記す。

この構成によるデータの転置装置の具体例を第６図に示す。この例ではＮ＝２４、Ｌ＝６、ｍ＝４である。以下にその動作を説明する。４個のブロックに分割されたデータは、まずブロック単位の転置（各ブロックの６個のデータをまとめて転置する。但し各ブロック内でのデータの順序は変更されない。）が同図(b)に示すブロック転置テーブルを用いて施される。例えばブロック１はブロック３の位置に、またブロック２はブロック１の位置に転置される。次にブロック転置されたデータはそれぞれ各ブロック毎に定められたデータ転置テーブル（同図(c)に示す）に従って各ブロック内で転置される。たとえばブロック１の位置に転置された各データは、転置テーブル１にしたがって転置される。

・テーブル容量

データ長Ｎ、データ長Ｌ、ブロック数ｍのデータ転置装置に必要な転置テーブルのメモリ容量は

$$M2 = m * [\log_2 m] + (m * L) * [\log_2 L] \text{（ビット）} \qquad (3)$$

である。内訳はブロック転置テーブルに

$$m * [\log_2 m] \text{（ビット）} \qquad (4)$$

と、各ブロック毎の転置テーブルに

$$L * [\log_2 L] \text{（ビット）} \qquad (5)$$

である。第６図の例（Ｎ＝２４、Ｌ＝６、ｍ＝４）

ではM2＝８０ビットとなる。また従来例１と比較するため、Ｎ＝６４、ｍ＝８の場合M2＝２１６ビットとなり、従来例１の５７％となる。このようにブロック数ｍをうまく選べば必要なメモリ容量を従来例１の約半分に削減できる。

・テーブル生成

従来例２の構成によるデータ転置装置では、

大きさｍの転置テーブル１個

大きさＬの転置テーブルｍ個

必要であるが、転置テーブルの大きさm，Ｌを$\sqrt{N}$（＜Ｎ）程度にすると、テーブル生成を従来例１と比較して容易にできる。つまりデータ長Ｎ＝６４の場合、従来例１では大きさ６４の転置テーブルが必要であったが、従来例２ではブロック数ｍ＝８とすることで、大きさ８のテーブルを５つ生成すればよい。

・安全性

従来例２において、選択されるべき転置規則の母集合の大きさは、簡単のため条件１を満たす規則を考えると

各ブロックの転置テーブルはそれぞれ大きさ

$$L!\qquad(7)$$

の転置規則の母集合から選ばれるため、この解読現実的に不可能にするためには式（７）を大きくしなければならない。

発明が解決しようとする課題

従来例１の構成によれば、転置テーブルの大きさを十分大きくとる必要があり、そのために生成時間が多大で、かつ一定でないため、頻繁に転置規則を更新させたい場合効率的でない。一方従来例２の構成によれば従来例１に比較して小さな（従来例１の大きさの平方根程度）転置テーブルで実現できるため、テーブルの生成時間を短縮でき、さらにメモリ容量も小さくすることが可能とされているが、前項で指摘したように各ブロック内で施されるデータの転置規則が転置されたデータの偏りから容易に推定される危険性があり安全性の面で好ましくない。

本発明は上述の問題点に鑑み試されたもので転置テーブルの生成時間及びテーブルのメモリ容量を従来例２程度にでき、かつ転置規則の推定を容易に行えないデータ転置を提供することを目的とする

$$m!*(L!)^m\qquad(6)$$

である。式（６）を転置規則を推定するのが困難なように設定する（但し実際は他の条件をも満たす転置規則の母集合の大きさを十分大きくする）。

例えばＮ＝６４、ｍ＝Ｌ＝８とすれば10^{38}程度となる。しかし、このようにＬとｍを設定しても以下に示す問題点から安全といえない。

第６図の例において、ブロック１に転置されたデータ（転置されたデータ系列の１～６番目のデータ）は元のデータ系列のブロック２のデータ（元のデータ系列の７～１２番目のデータ）を転置したものであることからも分かるように、この構成によれば、各ブロックのデータはそれぞれそのブロック内に偏って転置される。すなわち各ブロック毎に独立に転置規則を推定されるという危険性を有している。つまり転置データの各ブロックに対して転置規則を推定して、元のデータ系列の一部（ブロック）を復元し、次に、ブロック転置テーブルを推定して元のデータ系列を復元するといった解読が可能である。

課題を解決するための手段

本発明は上述した問題点を解決するため入力データ系列をブロックに分割する手段と、同一ブロックの各データをいくつかのグループに分配し配置する手段と、各グループに分配されたデータを各グループ内で転置する手段と、転置されたデータを各グループから収集し新たなブロックに配置する収集手段と得られたブロックを結合し転置データ系列を得る結合手段を備えたものである。

作用

本発明は分配手段が各ブロックに属するデータをいくつかのグループにランダムに分配配置することで各グループの属するデータは元のデータ系列に対してまったく偏りのないものにできるため、データ転置手段の各グループ毎に行う転置規則を容易に推定できないものとしている。

すなわちグループ毎に転置規則を解読できない構

成を取っている。またグループ毎の転置を施すことで必要な転置テーブルのメモリ容量を小さくできる。

実施例

第１図は本発明によるデータ転置装置の実施例である。同図において、１は本発明の構成によるデータ転置装置であり、以下の各部分から構成される。２はブロック分割部、３はデータ分配部、４はデータ転置部、５はデータ収集部、６はブロック結合部であり、７は入力データ格納部、８は出力データ格納部、９はデータ分配規則を格納するメモリ、１０は転置規則を格納する転置テーブル、１１は結合規則を格納するメモリである。

この転置装置の動作は以下の通りである。転置すべきデータ系列は、７の入力データ格納部に一旦格納され、２のブロック分割部に送られる。そしてそこで先頭から順次ブロックに分割される。次に各ブロックのデータはブロック毎に、３の分配部に送られ、そこで９の分配規則に従って、いくつかのグループに分配配置される。次に各グループに分配配置されたデータは４のデータ転置部に各グループ毎に送られ、１０の転置テーブルに従って転置される。各グループで転置されたデータは５の収集部で１０の収集規則に従って新たなブロックに収集され配置され、６のデータ結合部に送られ各ブロックが結合されて、８の出力データ格納部に格納される。そして最後に転置データ系列として出力される。なお分配規則メモリにはそのブロックの各データがどのグループのどの位置に配置するかが記述されている。また収集規則には各ブロックがどのグループのどの位置のデータを収集するかかが記述されている。以下で
N：データ長、m：ブロック数、L：ブロック長、k：グループ数、Qj（1≦j≦k）：グループ長、と記す。なお各グループ長を同一としてもよい。

第２図に上記構成による具体例を示す。同図に示す具体例は、N＝２４、m＝３、L＝８、k＝３、Q１＝９、Q２＝６、Q３＝９のデータ転置装置であり、その動作は以下の通りである。

２４個のデータはまず８個ずつ３個のブロックに分けられる。次に各ブロックの８個のデータは同図（ｂ）に示された分配規則に従って３個のグループに分配される（各ブロック共通にこの規則を用いる）。分配規則は次に示す通りとする。

ａ）メモリにはブロックの各データをどのグループに分配するかのみを記述し、各グループでの配置は、そのグループへの分配順序に従う。

例えば最初にグループ１に分配されるデータはブロック１の１番目のデータであり、それはグループ１の１番目に分配配置される。次にグループ１に分配されるデータはブロック１の４番目のデータでありそれがこのグループの２番目に分配される。

次に各グループ内でそれぞれ転置規則にしたがってデータ位置が転置される。例えば、グループ１のデータは転置規則１に従って、１番目のデータは４番目に、２番目のデータは５番目にというようにである。なお

ｂ）この例のように転置規則は左あるいは右巡回シフトで構成してもよい。

この場合転置テーブルのメモリ容量を減少できる（巡回するシフト量のみメモリに記述すればよい）。さらに、各グループのデータに対して、収集規則に従って各データが新たなブロックに収集される。収集規則は次の通りである。

ｃ）各グループの転置されたデータに対して分配規則とまったく逆の規則で各ブロックに収集した上で、左巡回シフトを施す。

例えばデータ分配部でブロック１の３番目のデータをグループ２の１番目に分配しているのに対し、分配部と逆の手順でグループ２の１番目に転置されたデータをブロック１の３番目のデータに配置するといった操作を全データに対した後に１だけこれを左に巡回シフトする（例えばブロック１の３番目に配置されたデータはブロック１の２番目に、ブロック２の１番目のデータはブロック１の９番目にブロック１の１番目のデータはブロック３の９番目にというようにである。）。なお収集

規則は

d）各グループをそのまま新たなとブロックとみなす。

ものとしてもよくこのばあい結合部では各ブロック（つまり各グループ）のデータを順次結合する。つまりグループ1の1～8の位置のデータの次にグループ2の1～8の位置のデータを結合するというようにである。

最後に各ブロックのデータは結合される。

・テーブル容量

データ長N、ブロック長L、ブロック数m、グループ数k、グループ長はそれぞれQj（すなわちQj（$1 \leq j \leq k$、$N=\Sigma Qj$）個ずつk個のグループに分配する）として必要なメモリは

$$M = L*[\log k] + k*[\log L] + \sum_{j=1\sim q} Qj\,[\log Qj] \quad (ビット) \quad (8)$$

となる。内訳はデータ分配規則格納用テーブルの容量は各ブロックのデータがどのグループに分配するかのみを規定すれば良いから

$$L*[\log k] \quad (ビット) \quad (9)$$

である。また各グループの転置テーブルに必要なメモリ容量は、

$$Qj*[\log Qj] \quad (ビット) \quad (10)$$

である。さらに結合規則としては、各グループのデータがどのブロックに収集するかのみを規定すれば良いから

$$k*[\log L] \quad (ビット) \quad (11)$$

となる。なお第6図の例では、M＝42ビットとなる。またN＝64、m＝L＝k＝Qj（$1 \leq j \leq 8$）＝8とすれば、M＝240ビットとなり、従来例1と比較して62％のメモリ容量となる。また従来例2と同程度となる（24ビット（収集規則メモリの容量分）増加する）。

・テーブルの生成

必要とする。この生成時間は従来例2と同程度と見積られる。この転置装置では

大きさLのテーブル1個

大きさQj（$1 \leq j \leq k$）のテーブル

大きさkのテーブル1個

（k，L、Qjは$\sqrt{N}$程度にできる）

必要とする。この生成時間は従来例2程度と見積られる。

・安全性

本構成によるデータの転置装置では元のデータ系列の各データを各グループにランダムに分配するため各グループ毎に解読を行っても元のデータ系列の1部分は復元できない。すなわち転置規則の解読を各グループ毎に独立には行えない。このため解読は本構成によってとり得るすべての転置規則について施さねばならない。従ってこの値を十分に大きく設定することで（例えば10^{30}以上）解読を不可能にできる。

具体例では実現可能な転置規則数は

$$k!*(Q!)^k \quad (12)$$

である。

発明の効果

以上の説明から明らかなように本発明は、データをグループに分配し、各グループで転置するという手段により、安全性の高いデータの転置を実現している。さらに、転置テーブルが容易に生成できるため、頻ばんに転置規則を変化させることが可能となる。またメモリ容量も従来例2程度にすることができる。

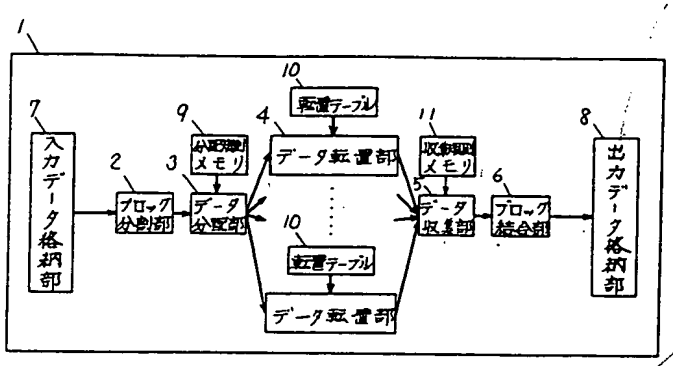
4．図面の簡単な説明

第1図は本発明によるデータ転置装置の実施例を示す構成図、第2図は同実施例における動作説明図、第3図は従来例1の転置装置を示す構成図、第4図は従来例1の動作説明図、第5図は従来例2の転置装置を示す構成図、第6図は従来例2の動作説明図である。

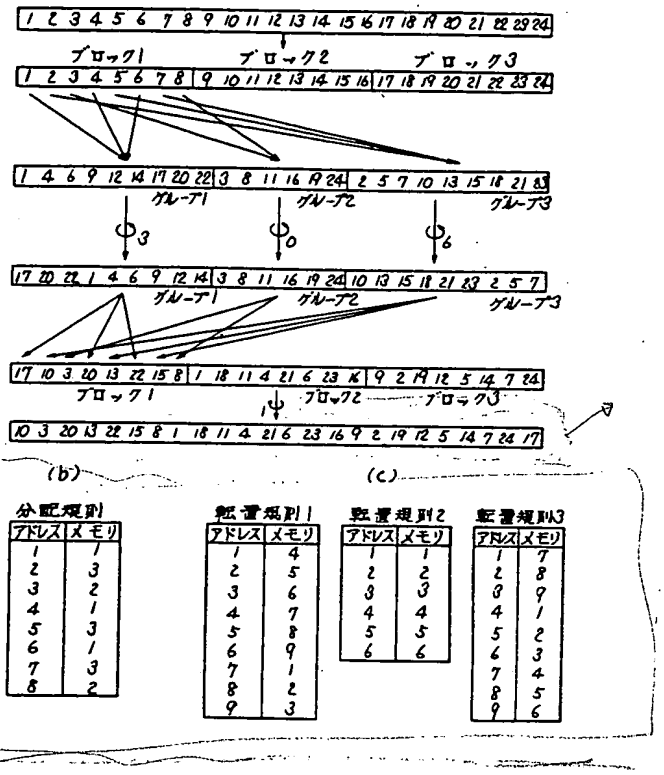
1…データ転置装置、2…ブロック分割部、3…データ分配部、4…データ転置部、5…データ収集部、6…データ結合部、7…入力データ格納部、8…出力データ格納部、9…データ分配規則を格納するメモリ、10…データ転置テーブルを格納するメモリ、11…データ結合規則を格納するメモリ。

代理人の氏名　弁理士　栗野重孝　ほか1名

第 1 図

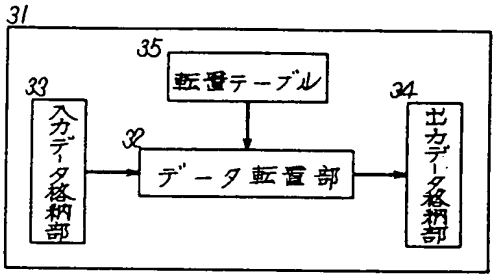


第 2 図



第 3 図

(a)



(b)

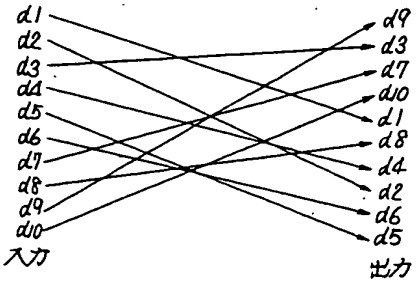
アドレス	メモリ
1	P_1
2	P_2
⋮	⋮
L	P_L
⋮	⋮
N	P_N

第 4 図

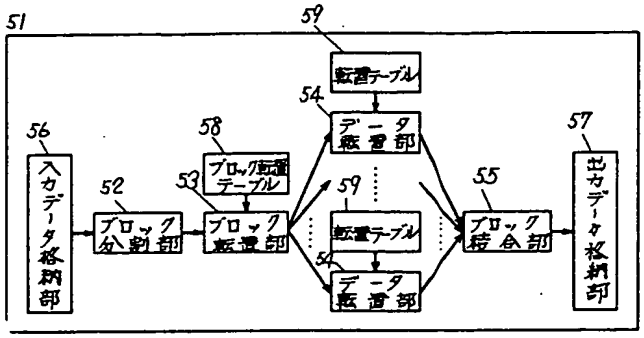
(a)

アドレス	メモリ
1	5
2	8
3	2
4	7
5	10
6	9
7	3
8	6
9	1
10	4

(b)

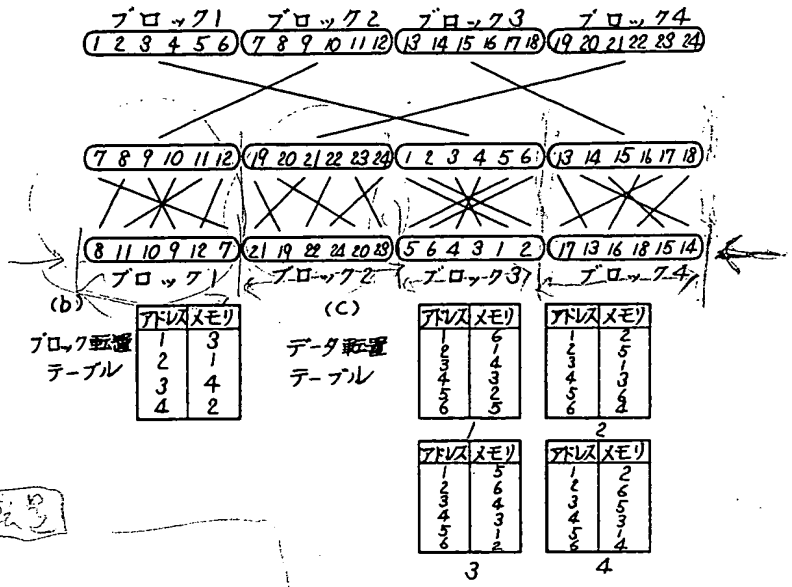


第 5 図


51
59
転置テーブル
54
データ転置部
56
入力データ格納部
58
ブロック転置テーブル
53
52
ブロック分割部
ブロック転置部
59
転置テーブル
55
ブロック結合部
57
出力データ格納部
54
データ転置部

第 6 図

(a)


ブロック1
ブロック2
ブロック3
ブロック4
1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17 18
19 20 21 22 23 24
7 8 9 10 11 12
19 20 21 22 23 24
1 2 3 4 5 6
13 14 15 16 17 18
8 11 10 9 12 7
21 19 22 24 20 23
5 6 4 3 1 2
17 13 16 18 15 14
ブロック1
ブロック2
ブロック3
ブロック4
(b)
ブロック転置テーブル
アドレス
メモリ
(c)
データ転置テーブル
2
3
4